PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04M — A2

(11) International Publication Number: **WO 98/17042**

(43) International Publication Date: 23 April 1998 (23.04.98)

(21) International Application Number: PCT/IL97/00329

(22) International Filing Date: 13 October 1997 (13.10.97)

(30) Priority Data:
119430 15 October 1996 (15.10.96) IL

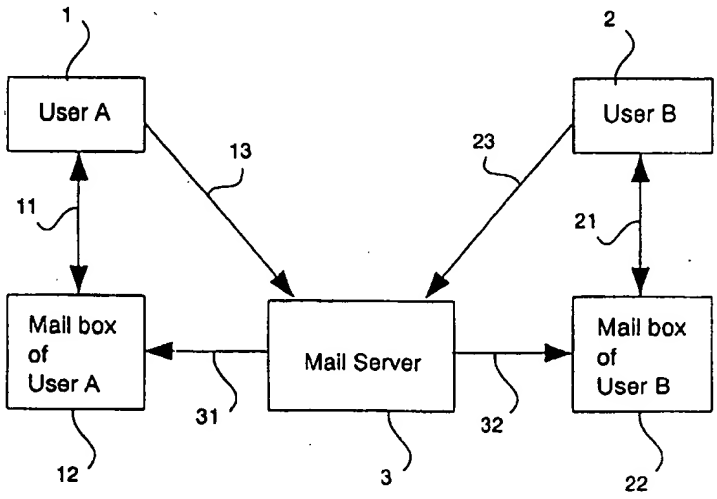
(71)(72) Applicant and Inventor: BARKAN, Mordhai [IL/IL]; Brande Street 24, 49600 Petah Tikva (IL).

(74) Agent: ZUTA, Mark; Ben Yehuda Street 19, 49373 Petah Tikva (IL).

(81) Designated States: AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: ELECTRONIC MAIL METHOD



(57) Abstract

A method for transferring electronic mail (E-mail) including registered and secure messages, uses means for achieving communications in which the sender receives proof of the E-mail message was indeed delivered to recipient. The recipient may either accept the message or not. A plurality of centers connected in a hierarchical key dissemination center array uses certificates to provide the public encryption keys to parties desiring to perform secure E-mail communications therebetween. The array also includes a plurality of intermediaries or post offices which can be used for legal registered mail (LRM). The method supports three modes of E-mail transmission: a secure message system, where there is not receipt of transmission; a business registered mail, where the transaction is direct between the parties and a receipt is returned to sender; and a legal registered mail, where an intermediary participates in the transaction to send the E-mail message to the second user and to bring a receipt to the first user.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

Electronic mail method

Technical Field

This invention concerns methods for transferring electronic mail.
The invention relates in particular to such methods which include means for transferring registered and secure messages.

Background Art

At present, various methods are used to transfer electronic mail, also known as E-mail.
A major drawback of prior art E-mail is that it operates "open loop" , that is the sender has no means for checking whether the recipient actually received the message.
The only possible way is to ask the recipient, which may be embarrassing and/or not in compliance with business etiquette.

This is an actual, real world problem. Sometimes messages do not reach the intended destination; at other times, errors occur during the communications, and the messages arrive unintelligible; at times, only part of a message is received. It may also happen that the message was received OK, but the recipient decided not to answer.

It may be of importance for the sender to know what actually happened, when there is no response to a given message. At present, there is no satisfactory answer to this need.
For business applications, this "open loop" property of E-mail may be a real disadvantage.

At present, there is a need to send "registered E-mail" , that is an E-mail message to be treated as registered mail, such that the sender receives proof that the message was delivered to its desired destination.
Even more important is proof of delivery for legal or formal mail. In these and a multitude of similar applications, proof of delivery may be mandatory.

There are practical problems in implementing an electronic version of the "registered mail" model.
One problem is the simultaneity of the "delivery of mail" and the "signature of receipt". In distributed systems, there can never be a simultaneous transaction. If the sender is the first to deliver the message, then a dishonest recipient may not acknowledge receipt (will not send the signed receipt to sender). If the recipient acknowledges receipt of the message prior to actually receiving it, then the sender may not send the message after all.

One proposed solution is the use of a trusted intermediary, or Post Office (PO). The PO accepts the message from sender and delivers it to recipient only after receiving the signed approval from recipient.

One problem with this approach is the huge amount of traffic in the PO, corresponding to the vast number of E-mail users. It is difficult to implement and maintain a PO capable of handling all this traffic.

Then there is the great responsibility on the PO. It may be sued if messages go wrong, so complex records of all transactions have to be kept for a long time.

Still another problem is the reliability of the PO itself. As a large number of messages pass through the PO, the PO becomes the weak link in all the E-mail communications. Unlike regular mail, E-mail may be opened or copied without leaving traces. It is difficult to ensure that the PO itself was not compromised.

Another attempt at a solution was proposed by Silvio Micali, as detailed in his article "Certified E-Mail with Invisible Post Offices" .
The parties exchange message and receipt which are encrypted with the public signature of a third party, the PO. Then the parties exchange the same, but en clair. If one party fails to perform, then the other may go to the PO which then acts to complete the transaction. The PO purportedly receives the required information to extract both message and receipt, and may complete the transaction by sending the missing document (message and/or receipt) to the other party. It is claimed that the PO can ensure that cheating is always detected.

A great disadvantage in Micali is that the recipient knows the identity of the sender, since the sender "Alice" indicates her identity and requires that "Bob" send the answer directly to her.

This is a definite departure from the "registered mail" model, where the recipient first has to sign a receipt, and only then gains knowledge of the sender's identity. One reason for that accepted procedure is that the knowledge of the sender's identity is in itself valuable information. By presenting it to recipient, the recipient gains an advantage without giving anything in return.

Another reason for the present method of registered mail is to prevent recipient to selectively accept/reject messages, according to the sender's identity. A sender may be interested to deliver a message to a reluctant recipient, for example a warning from the IRS or a warrant from a court of law. If the recipient is given the information who is the sender, then they may refuse to accept the message, so that a large part of the registered mail will never be delivered.

Thus, the method presented by Micali is not a true "registered mail" system.

Another disadvantage in Micali is that the recipient signs a message that he/she cannot read. This may leave open the possibility for attack, like by impersonation.

Still another disadvantage in Micali is that multiple copies of a message are sent back and forth, each with a different encryption. The same message is sent three times back and forth between the users.
This requires a complicated bookkeeping, to keep track of each message in both encrypted and en clair form.

Another disadvantage in Micali is that there is only one post office PO in the system, and that the PO must be trusted. Since E-mail is used on a huge scale worldwide, that PO will become eventually overloaded.
Moreover, it is required that all the people, worldwide, know that PO and its public key. What if the key has to be changed? There is no answer to that in Micali.

In E-mail systems, it may be desirable to present the recipient with the choice, whether he/she desires to receive the "registered E-mail" or not. Recipient should decide prior to his/her being presented with information regarding the identity of the sender or the contents of the message. This is similar to present registered mail, where letters should be signed for prior to disclosing the identity of the sender or the contents of the letter.

If the recipient decides to accept the message, then the system should allow the recipient to prove or sign that approval for the sender, and only then the message should be delivered to recipient.
This is impossible with present E-mail systems, where the message is delivered to recipient anyway, unconditionally; that is, the message is delivered to the recipient's electronic mailbox, without requiring their prior agreement.

Another problem is to ensure that the actual intended message reached the recipient. This problem is yet to be solved with registered mail, since at present there is only proof that an envelope was delivered to the recipient. There is no proof regarding the contents of that envelope.

The same need exists with respect to E-mail, that is to ensure or to prove that the intended actual message was delivered to its recipient.

Still another problem with E-mail is to achieve secure communications.
At present, various encryption devices and methods are used to encipher messages. All these devices assume that the parties involved had exchanged encryption keys prior to the encrypted communication session, such that both parties use the same key or complementary keys, as the need be.

There is a problem with secure key exchange between the parties, which is required to initiate the secure communications, and this is a vicious circle: Secure communications need an encryption key to be transmitted before that secure communication, but a secure communication link is required to transmit the key to begin with, otherwise the key is compromised and with it the whole subsequent encrypted communication.

A similar problem was addressed with my previous invention, Patent Application No. 113259, which was filed in Israel on April 5, 1995.
That invention cannot be applied to the present situation, since E-mail has different characteristics: While the previous invention detailed a real-time exchange between two parties, this is impossible with E-mail,
where each party has the equivalent of a mailbox, that is an address in a computer system into which other parties can write messages.

The recipient is not responding in real time or may, sometimes, decide not to respond at all. He/she may read the message from their mailbox at a later time, or may decide not to read it at all (for example when they are overflowed with messages, or when they decide to ignore old mail).

In other applications, there is a relationship of trust and cooperation between the parties, and the parties exchange messages as a routine.
Still, there is the requirement to acknowledge receipt, considering the occasional disruptions in communications, errors etc.
There is no method today for automatically acknowledging E-mail; with authentication of sender and receiver, and without requiring a trusted third party.

Thus, means are required for secure key dissemination for an E-mail communications environment, and/or relating to Internet.

The abovedetailed problems require of necessity a relatively complex solution; yet, the system should not be difficult to use, since E-mail, like regular mail, should be within the reach of people who are not experts in computer programming.

It is an objective of the present invention to provide for a registered and secure electronic mail system and method with means for overcoming the abovedetailed deficiencies.

Disclosure of Invention

It is an object of the present invention to provide a system and method for transferring electronic mail including registered and secure messages.
This object is achieved by an electronic mail method as disclosed in claim 1.
In accordance with the invention, the object is basically accomplished by providing an electronic mail method which includes means for achieving "closed loop" communications, that is communications in which the sender receives proof that the E-mail message was indeed delivered to recipient.

Novel system and method achieve communications similar or equivalent to "registered E-mail" .

It is another object of the present invention to provide means for presenting the recipient with the choice, whether he/she desires to receive the "registered E-mail" or not. If and only if the decision is positive, then proof of delivery is returned to sender, and the message is actually delivered to recipient.
Like with present registered mail, the information relating to the identity of the sender or the contents of the letter are made available to recipient only if he/she agrees to receive the E-mail message.

According to still another aspect of the present invention, the electronic mail system and method includes means for providing proof regarding the contents of the message received by recipient.

That is, sender get proof from recipient that the complete and unaltered message was received by recipient; the recipient can read the message only after giving this proof.

Furthermore, the electronic mail system and method includes means for achieving secure communications, that is the message being encrypted for preventing anyone en route from reading the message.

According to another aspect of the present invention, the electronic mail system and method includes a hierarchical key dissemination center array means using certificates to provide the encryption keys to parties desiring to perform secure E-mail communications therebetween.
The hierarchical key dissemination center array means may be used within the Internet environment.
The hierarchical array includes a plurality of key dissemination centers and post offices (PO) A user may select any post office for a specific transaction, thus eliminating a possible overload on any specific PO.

The electronic mail system and method includes means for performing the whole key exchange and communication session automatically, with minimal user intervention, both at the sender and the recipient ends.

The secure registered transmission may be performed between users which had no a priori arrangements for such transmissions, and over an open network like Internet or several interrelated networks.

For applications where there is a requirement to ensure the delivery of the message, the sender may choose a Legal Registered Mail (LRM) system, which makes use of a post office, but without placing too heavy a load on the post office.

For instances where there is cooperation between the parties, a less stringent delivery method may be chosen by sender, that is a Business Registered Mail (BRM), where the automatic transaction takes place between the parties without a post office or intermediary.

In any case, it is possible to implement a method where the message itself will not pass through the intermediary (the post office) so the weak link in the chain is avoided.

Moreover, there is no need to unconditionally trust the post office. According to the present invention, the post office may be interrogated and verified by the users, and/or the post office may be accessed anonymously to prevent a directed attack, towards a specific user.

Further objects, advantages and other features of the present invention will become obvious to those skilled in the art upon reading the disclosure set forth hereinafter.

Brief Description of Drawings

The invention will now be described by way of example and with reference to the accompanying drawings in which:

Fig. 1 details the structure of the registered E-mail delivery system.

Fig. 2 details the structure of a message prepared by the sender, during a first stage of a secure communication session.

Fig. 3 details the structure of the message after processing by a mail server, during a second stage of the communication session.

Fig. 4 details the structure of a message after processing by recipient, during a third stage of the communication session.

Fig. 5 details the structure of a hierarchical array including key dissemination centers, users and post offices.

Modes for Carrying out the Invention

A preferred embodiment of the present invention will now be described by way of example and with reference to the accompanying drawings.

Fig. 1 illustrates an example of a registered E-mail delivery system. Let's suppose user 1 desires to send a registered E-mail message to user 2. The designation "user 1" and "user A" are equivalent and will be interchangeably used throughout the present disclosure. Similarly, the terms "user 2" is equivalent to "user B" .

There are several methods of transmission which are available to user 1:

a) a secure message system, where the E-mail message is transmitted in encrypted form to user 2, without a receipt being sent back to user 1. The encryption key used for encryption may be retrieved from a key dissemination center which is part of a hierarchical array of centers, users and post offices. The array is detailed below with reference to Fig. 5 .

b) a business registered message system (BRM), where the E-mail message is sent encrypted to the second user, and an automatic algorithm at the second user returns a signed receipt if and when the second user agrees to receive the E-mail message.
Again, the encryption key used for encryption may be automatically retrieved from a key dissemination center which is part of a hierarchical array of centers, users and post offices, as detailed below with reference to Fig. 5 .

c) a legal registered message system (LRM), where an intermediary like a post office (PO) participates in the transaction to send the E-mail message to the second user and to bring a receipt to the first user.

Again, the encryption key used for encryption may be automatically retrieved from a key dissemination center which is part of a hierarchical array of centers, users and post offices, see Fig. 5 .

Referring to Fig. 1, user 1 has an electronic mailbox 12, which user 1 may access through communication link 11. For example, mailbox 12 may be a memory segment in a computer (not shown) of an Internet services provider (not shown). Link 11 may be implemented with any combination of a wide variety of communication means as known in the art, like telephone lines, wireless, local area network LAN and/or Internet links.

Similarly, user 2 has an electronic mailbox 22, which user 2 may access through communication link 21.

To implement the registered mail service, a mail server 3 is required. Mail server 3 may include a computer (not shown) or a plurality of computers, accessible through digital communication channels using any combination of a wide variety of communication means as detailed above. Each of the users 1 and 2 can send E-mail messages to mail server 3 through communication links 13 and 23, respectively. Communication links 13 and 23 are established with server 3 whenever a user desires to send a message to server 3.

Similarly, server 3 can send E-mail messages to each one of the users 1 and 2, through communication links 31 and 32, respectively.

To send a message to a user, server 3 actually accesses the electronic mailbox service provider for that user and sends a message to that mailbox.

Thus, Fig. 1 illustrates the structure of the system for registered E-mail transmission, wherein the communication links 13, 31, 23 and 32 exist only temporarily, being established at different times to convey the messages as required, to be detailed below.
A secure message may be transmitted as well.

Although only two users 1, 2 are depicted to explain the system, it is to be understood that a multitude of users can access the server 3 to concurrently transmit a multitude of registered mail messages.

The stages of the communication session are detailed with reference to Figs. 1, 2, 3 and 4, for the various transmission methods possible.

For the sake of clarity, the secure system will be detailed first, with the business registered mail (BRM) next, and the legal registered mail method (LRM) last.

Method 1

A secure electronic mail method for sending a first message from a first user 1 to a second user 2, comprises the following steps:

a. the first user 1 prepares the first message to be sent, indicates the identification of the second user 2 to whom the first message is to be sent, and activates an E-mail transmission program in their computer;

b. the E-mail transmission program at the first user 1 automatically connects to the Internet, connects there to one of the key distribution centers (for example center 63, see Fig. 5) and asks for the public key of the second user. The key dissemination array detailed in Fig. 5 is available to users on the Internet, so that each user can connect in real time to one of the centers 63, 62, 64 for example, and ask for the public key for another user;

c. the center 63 sends a certificate to the first user 1, wherein the certificate includes the public key for the second user 2 together with identifying information for the second user 2, all encrypted with the private key of the center 63. The certificate is akin to a statement like "The public key for the user 2 is abcd, and I center 63 hereby sign with my private key to attest to the truth of this statement" .

d. the E-mail program at the first user 1 decrypts the certificate to retrieve a public key for the second user 2;

e. the E-mail program at the first user 1 uses the public key for the second user 2 to encrypt the first message to be sent, to create a second message;

f. the E-mail program at the first user 1 sends the second message to the E-mail address 22 of the second user 2.

As mentioned above, there may be a plurality of key distribution centers like 63, 62, 61, 64 , and the E-mail transmission program can choose either one of the centers to ask for the certificate of the second user 2. The centers are preferably connected in a network which is hierarchical with respect to endorsement of the public key of each center, so that the public key of any center is endorsed in a certificate signed by the private key of a center higher in the hierarchy, up to one center at the highest level.

Thus, the public key of center 63 is endorsed in a certificate issued by center 62, and the public key of center 62 is endorsed by a certificate from center 61. Thus, the public key for any center is traceable to a higher authority, to achieve a reliable key system.

The system is also flexible, however, since any key can be changed without any detrimental effect on the system.

Moreover, in such a distributed key dissemination array with a plurality of key distribution centers, the E-mail transmission program for any user desiring to send an E-mail message can choose either one of the centers to ask for the certificate of a second user or addressee.

The centers are connected in a network capable of automatic exchange of certificates between the centers so as to locate a certificate for any desired second user which may be stored in any one of the centers, and for transferring the certificate to another center to be delivered to the first user.

Thus, for example (see Fig. 5), user 1 desiring to send a message to user 2 may connect to center 63. User 1 may choose center 1 for one of many reasons, like the center is close geographically to the user or known to them. When an inquiry regarding user 2 is placed with center 63, the inquiry is passed between centers 63, 62, 61, 64, 65. The information on user 2 is found at center 65, and a corresponding certificate is transferred on the same path in the reverse direction, back to center 63 and thence to user 1.

Thus, user 1 can inquire in real time about the public key for a desired addressee, and use that key for the subsequent E-mail transmission.

Unlike Micali, there is no overload on any specific center, since a plurality of centers is used and the workload is statistically divided therebetween.

Each center may be programmed to respond to any inquiry without requiring that the inquirer identify themselves. This prevents an attack by someone at the center, directed towards a specific user. This also allows to check the center by placing inquiries where the correct answer is known, to detect possible malfunctions at the center. Thus, the center need not be trusted, but can be verified by users.

Method 2

A secure method for sending a first message from a first user 1 (see Fig. 1) to a second user 2 as a business registered electronic mail (BRM), comprises the following steps:

a. the first user 1 prepares the first message to be sent, indicates the identification of the second user 2 to whom the first message is to be sent, and activates an E-mail transmission program in their computer;

b. the BRM E-mail transmission program at the first user 1 automatically connects to the Internet, connects there to one of the key distribution centers like center 63 or 62 or 64 (see Fig. 5) and asks for the public key of the second user 2;

c. the center 63 (if that center was selected for the transaction) sends a certificate to the first user 1, wherein the certificate includes the public key for the second user 2 together with identifying information for the second user 2, all encrypted with the private key of the center 63;

d. the E-mail program at the first user 1 decrypts the certificate to retrieve a public key for the second user 2;

e. the E-mail program at the first user 1 creates a second message which includes a message section including the first message to be sent which is encrypted with the public key for the second user 2, a hash or CRC of the message section, and a sender identification section with information to identify the first user 1;

f. the E-mail program at the first user 1 sends the second message to the E-mail address 22 of the second user 2;

g. when the second user 2 connects to Internet to retrieve messages in their E-mail 22, a BRM E-mail transmission program at the second user automatically presents information relating to the received second message;

h. the second user 2 is given a choice, either to accept or not the message. If the second user 2 decides not to accept the second message, then END; otherwise the E-mail program at the second user automatically decrypts the second message with the private key of the second user 2, presents the decrypted message to the second user 2, prepares a third message including a receipt for the second message signed with the private key of the second user 2, and sends the third message to the E-mail address 12 of the first user 1. The receipt includes the identification of the message and the received hash or CRC, so the second user 2 signs to approve receipt of a specific message, and that the message was received in full.

In the above Method 2, the public key of user 2 may be used directly to encrypt the message, or indirectly. In an indirect implementation, the message itself is encrypted with a symmetrical key and algorithm, and the corresponding decryption key is separately encrypted with the public key of user 2.

The same key may be used both for encryption and decryption, for example using XOR logic with a random string derived from the key, or the DES algorithm.

In one embodiment of the above Method 2, the sender identification section in the second message (the message prepared in step (e) at the first user) may include a certificate with the public key of the first user 1, signed by a key distribution center like center 63. User 1 may store their certificate from center 63, and present the certificate to any second party for establishing their identity. The other party may choose to accept that certificate, or ask in real time for an updated certificate for user 1, from one of the key distribution centers like centers 62, 63.

The whole transaction of certificate transmission, acceptance and verification is done automatically by the E-mail program at the first and second user, without user's intervention (unless the user chooses to intervene and override the automatic process).
This achieves a fast and secure transaction, which is also easy to use.

In another embodiment of the above Method 2, the sender identification section in the second message (the message prepared in step (e) at the first user) may include a name or pseudonym which identifies the first user 1.

The second message further includes a general information section comprising a CRC or hash and/or other information, all encrypted with the private key of the first user; and wherein the E-mail program in the second user automatically connects to a key distribution center to retrieve the public key of the first user, which key is used to decrypt the general information section; if the CRC or hash and/or the other information therein corresponds to that computed by the E-mail of the second user, then will the second user send the third message to the first user.

It is possible to use Method 2 where there are a plurality of key distribution centers like centers 61, 62, 63 (see Fig. 5) and the E-mail transmission program can choose either one of the centers to ask for the certificate of the second user 2, and wherein the centers are connected in a network which is hierarchical with respect to endorsement of the public key of each center, so that the public key of any center is endorsed in a certificate signed by the private key of a center higher in the hierarchy, up to one center at the highest level.
Thus, center 62 attests for the public key of center 62, center 61 attests for center 62 etc.

Thus, the BRM method in the present disclosure allows for an integrated approach, using concurrently an on-line, real-time connection (to the key distribution center) and a non-real time connection (with the E-mail addressee). The public key is retrieved automatically using the distributed key centers array.

Method 3

A secure method for sending a first message from a first user to a second user as a legal registered electronic mail (LRM), comprises the following steps:

a. the first user 1 (see Fig. 1) prepares the first message to be sent, indicates the identification of the second user 2 to whom the first message is to be sent and an intermediary or post office (PO) for the transmission (like post office 71 or 72, see Fig. 5). The first user then activates an E-mail transmission program in their computer;

b. the LRM E-mail transmission program at the first user 1 automatically prepares a second message including the first message which is encrypted for example with a symmetrical key and algorithm, together with a general information section including a serial number or message identification and information relating to the public key of the second user 2, together with a CRC or hash and optional time/date information.

c. the LRM E-mail transmission program at the first user 1 automatically prepares a third message including the decryption key for the first message, encrypted with the public key of the second user 2, together with a general information section including a serial number or message identification, together with the CRC or hash and optional time/date information;

d. the LRM E-mail transmission program at the first user 1 automatically prepares a fourth message including a notice that an E-mail message was sent to the second user, the CRC or hash of the message, the identification of the intermediary 71 and the serial number or message identification;

e. the LRM E-mail transmission program at the first user 1 sends the third message to the chosen intermediary or PO 71, the fourth message to the second user 2 and the second message either to the intermediary 71 or the second user 2;

f. when the second user 2 connects to Internet to retrieve messages in their E-mail 22, a LRM E-mail transmission program at the second user automatically presents information relating to the received message;

g. the second user 2 is given a choice, either to accept or not the message. If the second user 2 decides not to accept the second message, then END; otherwise the E-mail program at the second user 2 automatically encrypts the fourth message with the private key of the second user 2 to create a fifth message, and sends the fifth message to the intermediary or PO 71, so that the fifth message is a receipt signed by the second user 2, with the receipt including the message identification and the CRC or hash relating to the contents of the message.

h. the intermediary 71 decrypts the fifth message with a public key of the second user 2, and compares with the message identification in the third message; if the two correspond, then the intermediary sends

the third message with the decryption key therein to the second user 2, and the fifth message with the receipt from the second user is made available to the first user 1; if the second message with the encrypted message itself was sent to the intermediary 71, then the intermediary 71 sends the second message to the second user 2.

An advantage of the above Method 3 over Micali and others is that there are a plurality of intermediaries or post offices (PO) like 71, 72, 74. Any user with a computer and suitable software may act as a post office, provided they connect in the hierarchical array and can use and present a public key endorsed by a key distribution center. The endorsement is usually in the form of a certificate. Thus, the overload on a single center is eliminated. Users worldwide can each select any PO for any given transaction. Moreover, the PO has no motivation to cheat the user who selected that PO, and may later select other PO if not satisfied.

The PO need not be trusted, but can be interrogated and tested by any user, for example by sending E-mail to themselves at a different E-mail address or pseudonym.

Thus, in the above Method 3, there may be a plurality of intermediaries or POs like 71, 72, 74 (see Fig. 5), and the E-mail transmission program can choose either one of the intermediaries to act as PO for a given transmission.

The intermediaries or POs may be connected in a network which is hierarchical with respect to endorsement of the public key of each center and intermediary, so that the public key of any intermediary is endorsed by a certificate issued by a key distribution center like center 63, 62, 65 etc.
The public key of each center is endorsed in a certificate signed by the private key of a center higher in the hierarchy, up to one center at the highest level.

Moreover, in the above Method 3, the LRM E-mail transmission program at the first user 1 may automatically extract the public key for the intermediary 71 and/or the second user 2 by connecting to a key distribution center like center 62 on Internet and asking for a certificate for the intermediary 71 and/or second user 2. The public key thus obtained and contained in a certificate or certificates from center 62 is/are most updated and reliable.

These reliable public keys may be used in the subsequent transaction with the entity (second user, intermediary) to which that key belongs.

In another embodiment of the present invention, the LRM E-mail transmission program at the second user 2 automatically challenges the intermediary 71 for its key by receiving a message encrypted with the private key of the intermediary 71 and decrypting with the public key thereof.

This is used to ensure that the receipt is sent to the real intermediary 71, not to an impostor.
Thus, the fifth message in step (g) is sent to the intermediary or PO 71 only if the keys of the intermediary 71 correspond.

There are two variants of Method 3, in one the encrypted actual message is sent directly to the second user 2, and in the other the message is sent to the intermediary 71. Each variant has its advantages.

The first variant demands less overload on the intermediaries like 71, 72 since the intermediaries only handle the keys which comprise short messages. The bulk of the communications is in the messages, and these are transferred directly to user 2.

The second variant may be attractive where there is a requirement to keep a log of E-mail transactions at an objective party, for example in a key escrow.
If and when there is a legal framework to govern electronic transactions, the system and method of LRM disclosed in the present invention may support the legal requirements of the law. An intermediary like 71, 72 will keep a log of all message, to allow subsequent verification and to preserve the security of the system.

Figs. 2, 3 and 4 detail the structure of messages in the various parts of the system as detailed above for a legal registered mail (LRM) system and during the several stages of the communication session to be detailed next.

Method 4

To send a registered secure message from user 1 to user 2, the communication session includes the following stages:

a. User 1 prepares an encrypted message which includes, see Fig. 2 :

1) the message section 41, including the message to be send, encrypted with a symmetrical key and algorithm (this is a method using the same key both for encryption and decryption, for example using XOR logic with a random string derived from the key, or the DES algorithm). User 1 generates a new randomial symmetrical key for each message to be transmitted. Thus, the message 41 can be read only by someone possessing the required symmetrical key.

2) the decryption key section 42, comprising the symmetrical key which is to be used to decrypt the message in section 41, which key itself is encrypted using a public key algorithm with the public key of user 2.

Thus, only user 2 can open section 41 of the message, since only user 2 possesses the private key with which section 42 can be opened or decrypted, to reveal the symmetrical key within.
This protects the message in section 41 from being read by anyone in the whole communication channel from user 1 to user 2.

3) the CRC section 43, which is used for sender authentication purposes. It includes a cyclic redundancy code or CRC which is derived from the message being sent in section 41, and encrypted with the private key of user 1. This is the de facto signature of user 1, since anyone can compute the CRC, and compare it with its encrypted version as received, after being decrypted with the public key of user 1. If the two values are identical, this is proof that user 1 prepared and sent the message. Either a CRC or a hash may be used, without departing from the spirit and scope of the present invention.

4) sender identification section 44, including the name, address and/or other information identifying user 1. May be sent en plain.

5) recipient identification section 45, including the name, address and/or other information identifying user 2. May be sent en plain.

The encrypted sections 41, 42, 43 form the first layer of encryption 51, see Fig. 2 .

In another embodiment of the invention, only section 42 is encrypted. This saves part of the computational effort, and prevents section 41 from being encrypted twice.

b. user 1 sends the encrypted message as detailed in (a) above to mail server 3 through link 13 (see Fig. 1).

c. mail server 3 processes the message to create a new message derived from the received message and which includes, see Fig. 3 :

1) the message section 41, as received. Server 3 cannot read the message in section 41, since it is encrypted. Server 3 also cannot read the key to decrypt the message, since the key section 42 is encrypted as well, such that only user 2 can read it.

2) the decryption key section 42, encrypted with a second symmetrical key and algorithm, with a second key generated in server 3. Server 3 generates a new randomial symmetrical key for each message to be transmitted.
In another embodiment of the invention, it is possible to encrypt the whole message, not only parts of it.

Thus, the decryption key in section 42 can be read by user 2 only if given the second key generated in server 3.
This prevents the message in section 41 from being read by user 2 until given the second symmetrical key from server 3.

3) the CRC section 43, as received.

4) sender identification section 44, encrypted with the same second symmetrical key and algorithm, with a second key generated in server 3. Thus, user 2 is prevented from gain access to the sender, that is user 1, identification until being given the second symmetrical key.

5) recipient identification section 45, as received.

6) a message identification number or alphanumeric string 46, which unambiguously identifies each message sent by server 3. That number is used by server 3 to identify each registered message being processed in the system.

The encrypted sections 42, 44 form the second layer of encryption 52, see Fig. 3 .

d. mail server 3 sends the encrypted message as detailed in (c) above to user 2 through link 32 (see Fig. 1). Actually, the message is sent to the mailbox 22 belonging to user 2.

e. user 2 reads his/her E-mail from the mailbox 22, through link 21. There is indication that a registered E-mail message arrived which is addressed to user 2, and a number to identify the message with the server 3.

User 2 however, cannot read the message or find the identity of the sender. This is identical to the method used in regular registered mail.

f. User 2 is given the choice of either to accept or not to accept the registered mail.

1) If user 2 declines to accept the message, then he/she cannot gain access to its contents, thus for all practical purposes the message is not delivered. Server 3 may send "second notice" remainders, according to a routine to be established, then the message will be considered as undelivered. Notice may be send to the first user that the message could not be delivered.
The transaction ends here.

2) If user 2 decides to accept the message, then the computer of user 2 prepares a response message as follows: the whole message or only a hash of the message or a CRC thereof is encrypted using a public key method, with the private key of user 2.
This is the message detailed in Fig. 4.

This encryption by user 2 serves as the signature of user 2 to the effect that he/she agrees to accept the registered E-mail message. Since only user 2 can use their private key, this serves as authentication of user 2's confirmation of the registered mail delivery.

Moreover, since user 2 signs (by using their private key) for the whole document, this is proof that the whole document was received OK. This is a much stronger proof than that of ordinary registered mail, where there is only proof that a package was delivered, but there is no proof regarding the actual message that was received by the other party.

The encrypted message with the private key of user 2 forms the third layer of encryption 53, see Fig. 4 .

g. User 2 sends the encrypted message prepared as detailed in f(2) above to server 3 through link 23 (see Fig. 1).

h. mail server 3 decrypts the message prepared as detailed in f(2) above, using the public key of user 2. The decrypted message is compared with the message sent to user 2, as illustrated in Fig. 3 .

1) If the two are identical, this is proof that user 2 agrees to receive the registered E-mail message. This is also proof that user 2 received correctly the complete message from user 1.

In this case (the messages are identical):

Mail server 3 sends the second symmetrical key to user 2, see Fig. 3 . This enables user 2 to open the registered mail message.

Mail server 3 also sends to user 1 a message including the encrypted message from user 2, see Fig. 4, concurrently with the transmission of the second symmetrical key to user 2.
The message to user 1 is sent through link 31 (see Fig. 1). Actually, the message is sent to the mailbox 12 belonging to user 1.
Similarly, the message to user 2 is sent to mailbox 22 through link 32.

2) If the two messages are not identical, this may indicate that an error occurred during the transmission, in which case additional attempts at sending the message to user may be made, that is step (d) above is performed again.
It may also indicate that the message has not been sent to the right address; this is to be verified as well.

i. User 2 can now open the E-mail message, as follows:

1) the decryption key section 42 is opened using the second symmetrical key received from server 3, see step h(1). This reveals the original section 42 which was prepared by user 1.

2) the sender identification section 44 is also opened using the second symmetrical key received from server 3. This reveals the sender, that is user 1, identification, including the name, address and/or other information identifying user 1.

3) the message section 41 is decrypted using the decryption key which was opened in step i(1) above. Thus the E-mail message finally reaches its destination.

4) the CRC section 43 is opened using the public key of user 1. A second CRC is computed for decrypted message in step i(3), and the two CRC s are compared. If they are identical, this may be used sender authentication purposes. This proves that user 1 indeed is the sender of the message.

j. User 1 has proof that the message was delivered to its destination:

1) the message from server 3, including the encrypted message from user 2, see Fig. 4, is opened using the public key of user 2, to reveal the message sent to user 2 by server 3, see Fig. 3.

2) the message thus opened is compared with the original message sent by user 1, see step (b) above. If the two messages are identical, then user 1 has proof that user 2 received the message as sent, since user 2 signed it with his/her private key. This is also proof that the contents of the message was delivered, not only the "package" or "envelope" which contains the message.

k. User 1 may send notice to server 3 according to the results of the comparison made in step j(2) above:

1) If the messages are identical, server 3 is noticed to that effect. Server 3 can then delete all the files relating to the transaction, except maybe some details for later referral.

2) if the messages are different, then server 3 can check the various messages to detect the source of the error and/or try again to complete successfully the registered E-mail delivery.

Method 5

The abovedetailed registered secure E-mail transmission may be performed automatically, with minimal users' intervention, as follows:

a2. user 1 prepares the message to be send, and initiates the registered secure E-mail transmission, for example by activating an icon or pushing a button on screen, which icon or button has assigned the function "send registered secure E-mail" therewith.
This is the first manual action performed in the transmission process.

b2. the computer at user 1's location automatically performs the steps (a) and (b) above

c2. the computer at server 3 location automatically performs the steps (c) and (d) above.

d2. user 2 finds there is a registered encrypted message waiting in his/her mailbox 22. If user 2 decides to accept that message, then he/she indicates that agreement, for example by activating an icon or pushing a button on screen, which icon or button has assigned the function "accept registered secure E-mail" therewith. This action has the effect of user 2 signing for the registered mail acceptance.

This is the second and last manual action performed in the transmission process.

These steps represent steps (e) and (f) above.

e2. the computer at user 2's location automatically performs the step (g) above.

f2. the computer at server 3 location automatically performs the step (h) above.

g2. the computer at user 2's location automatically performs the step (i) above, to bring and present the complete received message to user 2.

h2. the computer at user 1's location automatically performs the steps (j) and (k) above, to indicate to user 1 that the message was received successfully and that proof is in the records of user 1's

computer, or that the message was not delivered and adequate actions are being taken.

The above description assumed that each user knows the public key of the other, as well as the public key for server 3. If the key is not known or the user has an obsolete key, then a key dissemination center array may be used for that purpose.

Fig. 5 details the structure of a hierarchical key dissemination (K. D.) center array means.

These K.D. centers are used to create and exchange certificates including a secure key between the parties, such that each user gains access to an updated key, with the knowledge that that is truly the key belonging to the user as desired.

For example, user 1 asking for the public key for user 2, will access its key dissemination center 63. Center 63 is connected in a hierarchical array with other centers, depicted here as 61, 62, 64, 65.
The hierarchical structure is for net.structure definition only; the actual operation is that of a flat distributed network, in which each of the centers 61, 62, 63, 64, 65 can directly reach each other of said centers.

Each user in the system has an unique identification number or name or address, akin to the telephone number or Internet address. Part of that identification number indicates the center that user belongs to.

Thus, while user 1 asks its center 63 about the key for user 2, center 63 can determine from the number for user 2 that user 2 belongs to center 65. Actually each of the centers 61, 62, 63, 64, 65 has a table indicating which center should be accessed for each user number possible.

Having thus determined that the required key is to be found in center 65, center 63 automatically accesses that center, extracts the key for user 2 and delivers it to user 1.

Method 6

To protect the whole sequence, a public key encryption algorithm is used, as follows:

a3. The computer at user 1's facility automatically connects the secure encryption key distribution center 65, and sends an inquiry message asking for the public key for the addressee, user 2 in this example, the message being encrypted with the public key for center 63.

b3. Center 63 decrypts the message, verifying the identity of user 1 in the process; the answer is sent to user 1, encrypted with the public key for that user. The center 63 maintains a list of public keys for its various users like 1, 73 in this example.

c3. User 1 can now access user 2, to send the E-mail message as detailed above.
Center 63 accesses center 65 to get the key for user 2, using a similar encryption procedure, to ensure the secrecy and integrity of the process.

In another implementation, center 65 creates a "certificate" , that is a message including the public key for user 2, together with identification information for user 2, all encrypted with the private key of center 63. Anyone, for example user 1 or 2, can ask for a certificate on any other user or for himself; the certificate can be opened by anyone using the known public key for center 65, thus ensuring the authenticity of the key.
The key of center 65 can be verified using centers higher in the hierarchy like centers 64 and 61.

While sending an encrypted message, user 1 can attach his own "certificate" to that message, to facilitate its decryption by the addressee.

Thus, there is provided a system and method for transferring electronic mail including registered and secure messages.

The method is automatic, with minimal users' intervention. It can be performed between users which did not know each other before, over an open network like Internet.

Various implementations of the abovedetailed system and method will become apparent to persons skilled in the art.

For example, server 3 may encrypt the whole message, see Fig. 2, and not only the sections as detailed.

User 1 may encrypt the whole message with the public key for server 3, for additional protection and/or to prevent anyone from tampering with the message. User 2 may encrypt messages to server 3 as well.

This system has the additional advantage that it helps fight the nuisance of "junk mail" , that is the mailbox being filled with unsolicited and unwanted messages. The user can select to consider first the registered E-mail messages, which may be believed to be of more use. If there is a fee to be paid to send registered mail, that may discourage "junk mail" senders from using this method.

Method 7

It is also possible to use a variant of Method 6 above which requires less effort on the side of the mail server, or post office PO.

This is the Legal Registered Mail (LRM) system, which makes use of a post office, but without placing too heavy a load on the post office.

In this method, the message is sent directly to user 2, encrypted. The key required to decrypt it is sent through the PO.
Thus, user 2 still has to acknowledge receipt of the message to receive the decryption key therefor. However, in this case the PO is not required to store and handle the whole message, but only the keys. Another advantage of this method is that the PO has no access to the messages themselves, so that the PO cannot compromise the message.

To send a registered secure message from user 1 to user 2, the communication session includes the following stages:

a. User 1 prepares a first encrypted message which includes :

1) the message to be send, encrypted with a symmetrical key and algorithm (this is a method using the same key both for encryption and decryption, for example using XOR logic with a random string derived from the key, or the DES algorithm).

User 1 generates a new randomial symmetrical key for each message to be transmitted.

2) a serial number or identification number for the message. This will be used later by all the parties to identify each specific message being processed, taking into account that each party may concurrently handle many messages.
This number may be sent en clair or may be encrypted with the public key of user 2.

3) (optional) a CRC or hash of the encrypted message being sent, as prepared in (1) above. The CRC may include the serial number in (2) above.

4) (optional) the indication of the intermediary or post office where the decryption key is available. In another implementation, the users use a common or local or otherwise obvious post office, and no such indication may be necessary.

b. User 1 sends the first encrypted message to user 2, directly.

c. User 1 prepares a second encrypted message which includes :

1) the decryption key, comprising the symmetrical key which is to be used to decrypt the message being sent to user 2, which key itself is encrypted using a public key algorithm with the public key of the post office.

Optionally, the decryption key may be first encrypted with the public key of user 2, then encrypted with the public key of the PO in a second stage or layer of encryption.
This provides an additional level of security, since the PO cannot read the decryption key. This is not mandatory, however, since the PO has no access to the message itself, which is sent directly to user 2.

2) the serial number or identification number for the message. This will be used later by all the parties to identify each specific message being processed, taking into account that each party may concurrently handle many messages.
This number may be sent en clair or may be encrypted with the public key of the intermediary or post office.

3) (optional) a CRC or hash of the encrypted message being sent, as prepared in a(1) above. The CRC may include the serial number in a(2) above. This allows the post office to ensure the receipt of the correct message by user 2, prior to releasing the decryption key.

Note: throughout the present disclosure, CRC and hash are used interchangeably. In the actual implementation, each of the two may be used, according to relevant consideration like the computational effort required, response time, safety required etc.

4) (optional) the indication of the identity of user 2, who is expected to claim the "mail" , that is the key to decrypt it.
This is not mandatory, since there is a measure of safety already – only user 2 can read the serial number of the message (if it was encrypted with their public key), so only user 2 will know to ask for the "package" with that number.

Moreover, the decryption key itself is encrypted with the public key of user 2, so an impostor will not be able to decrypt the package and extract the decryption key therein.
Still, the capability to identify user 2 by the post office adds another level of security.

d. User 1 sends the second encrypted message to the post office PO.

e. user 2 reads his/her E-mail from the mailbox.
There is indication that a registered E-mail message arrived which is addressed to user 2, and a number to identify the message with the intermediary or post office. User 2 however, cannot read the message or find the identity of the sender. This is identical to the method used in regular registered mail.

f. User 2 is given the choice of either to accept or not to accept the registered mail.

1) If user 2 declines to accept the message, then he/she cannot gain access to its contents. thus for all practical purposes the message is not delivered. The post office PO may send "second notice" remainders, according to a routine to be established, then the message will be considered as undelivered. The PO may notify the first user that the message could not be delivered.
The transaction ends here.

2) If user 2 decides to accept the message, then the computer of user 2 prepares a response message as follows: An acknowledgment of receipt is composed, including the serial number of the package and additional optional information, all encrypted using a public key method, with the private key of user 2.

Optionally, the message includes a CRC of the whole message as well, in case the method in use requires confirmation of receipt of the correct message by user 2.

This encryption by user 2 serves as the signature of user 2 to the effect that he/she agrees to accept the registered E-mail message. Since only user 2 can use their private key, this serves as authentication of user 2's confirmation of the registered mail delivery.

Moreover, since user 2 signs (by using their private key) for the CRC of the whole document, this is proof that the whole document was received OK.

This is a much stronger proof than that of ordinary registered mail, where there is only proof that a package was delivered, but there is no proof regarding the actual message that was received by the other party.

g. User 2 sends the encrypted message prepared as detailed in f(2) above to the post office.

h. the post office decrypts the message prepared as detailed in f(2) above, using the public key of user 2. The decrypted message is compared with the message sent to user 2.
If the serial number of the package corresponds to that sent by user 1, this is proof or signature of receipt of package by user 2.
The post office may then send the decryption key (the second message, prepared in step (c) above by user 1) to user 2. The receipt from user 2 is sent back to user 1.

If it is required to confirm receipt of the correct message, then the post office may compare the CRC received from user 2 (computed in step f(2) above) with the CRC computed by user 1 (computed in step c(3) above). Only if the two CRCs correspond, will the decryption key be sent to user 2.

Otherwise, the post office may notify both users that an error occurred during transmission, so recovery measures may be taken, for example by cancellation of the message and retransmit.

i. User 2 can now open the E-mail message, as follows:

1) the decryption key is opened using the private key of user 2.

2) the decryption key is used to decrypt the message.

j. User 1 has proof that the message was delivered to its destination:

1) the message from the post office, including the encrypted message from user 2 is opened using the public key of user 2, to reveal the message sent to user 2 by the post office.

2) the message thus opened is compared with the original message sent by user 1. If the two messages are identical, then user 1 has proof that user 2 received the message as sent, since user 2 signed it with his/her private key. This is also proof that the contents of the message was delivered, not only the "package" or "envelope" which contains the message.

An advantage of the abovedetailed Method 4 for the Legal Registered Mail (LRM) system is that the post office need not be trusted.

There are several safety means to protect the E-mail messages. For one, the post office has no access to the messages, since the message is transferred directly to user 2. So, the post office cannot use the key to decrypt the message being sent.
As another safety means, the decryption key is also encrypted with the public key of user 2, thus the decryption key cannot be read at the post office.

Furthermore, the identification of the users before the post office is optional. In a higher security system, users 1 and 2 retain their anonymity. The post office cannot mount an attack on a specific user or target, since the post office will now know the identity of the users.
It also makes it the more difficult for a malicious person to find where is the message itself, since they will not know the identity of the users at all.

Another advantage of sending the message directly to the second user is that the workload on the PO is greatly reduced. There is no need for the PO to handle large amounts of traffic corresponding to the messages themselves. The keys messages result in a vastly reduced traffic. Thus, a problem in prior art that a PO may be blocked because of the high volume of traffic, is solved in the present invention.

Moreover, each user can verify the post office, for example by anonymously sending a package and then demanding it, using a different pair of keys for example. If the post office is not working proper, then this may be detected by users.
Thus, users making inquiries on the post office randomly act as a watchdog to ensure/verify the integrity of the post office.

In another implementation of the present invention, for instances where there is cooperation between the parties, a less stringent delivery method may be chosen by sender, that is a Business Registered Mail (BRM). Following is a description of this method, Method 8.

Method 8

This is a method usable between cooperating parties, the Business Registered Mail (BRM) system. The method is secure in the sense that other parties cannot gain access to messages. There are, however, no security means to protect one party to the communication from the other party, since this is deemed not necessary because of the cooperating nature of the relationship therebetween.

To send a registered secure message from user 1 to user 2, the communication session includes the following stages:

a. User 1 prepares a first encrypted message which includes :

1) the message to be send.

2) sender and recipient identification

3) a serial number or identification number for the message.

A time and date information may be used in lieu of the serial number, or in addition thereto.

4) (optional) a CRC or hash of the encrypted message being sent.

The message may be encrypted with the public key of user 2.

In another embodiment, the message is encrypted with a symmetric key, and a second section is added to the message, where the second section includes the decryption key, encrypted with the public key of user 2.

The hash or CRC may be encrypted with the private key of user 1, so as to serve as their signature on the complete document.

b. User 1 sends the first encrypted message to user 2, directly.

c. user 2 reads his/her E-mail from the mailbox.

There is indication that a registered E-mail message arrived which is addressed to user 2. User 2 decrypts the message using their private key.

The CRC is computed, to verify correct receipt of the message.

d. A response message is composed. It may include the serial number and/or date and time of the message as sent, the time and date it was received, and a flag to indicate that the reception was OK or not, based on the comparison of the CRC in the message with the computed CRC. The whole message may be encrypted with the public key of user 1, to prevent the information relating to the message from being read by others.

Optionally, the message is further signed or encrypted with the private key of user 2, so that user 1 has proof that the message was received correctly by user 2.

e. The response prepared in (d) is sent to user 1, to acknowledge receipt. Thus user 1 receives confirmation regarding the receipt of the message.

f. User 1 is presented with the information regarding the delivery of the message, together with the status of all the other messages sent. The presentation is performed at the user's computer. Thus the user can keep track of all the messages being sent to all the other users.

In a preferred embodiment of the invention, the user has a choice to select the communication method, as detailed in Method 8 below.

Method 9

1. The user's computer presents a menu to the user whenever the user desires to transmit an E-mail message. The menu includes the various method of transmission.

2. The user may choose to send the message en clair or using the BRM method or the LRM method, according to circumstances. The method may depend on the nature/sensitivity of the message itself, and/or the nature of the relationship with the recipient.
The user chooses from the menu accordingly.

3. The E-mail program in the computer activates a corresponding routine, to implement either one of the communication methods as detailed above, for example the BRM or LRM method.

It will be recognized that the foregoing is but one example of an apparatus and method within the scope of the present invention and that various modifications will occur to those skilled in the art upon reading the disclosure set forth hereinbefore

CLAIMS

1. A secure electronic mail method for sending a first message from a first user to a second user, comprising the following steps:

a. the first user prepares the first message to be sent, indicates the identification of the second user to whom the first message is to be sent, and activates an E-mail transmission program in their computer;

b. the E-mail transmission program at the first user automatically connects to the Internet, connects there to one of the key distribution centers and asks for the public key of the second user;

c. the center sends a certificate to the first user, wherein the certificate includes the public key for the second user together with identifying information for the second user, all encrypted with the private key of the center;

d. the E-mail program at the first user decrypts the certificate to retrieve a public key for the second user;

e. the E-mail program at the first user uses the public key for the second user to encrypt the first message to be sent, to create a second message;

f. the E-mail program at the first user sends the second message to the E-mail address of the second user.

2. The secure electronic mail method according to claim 1, wherein there are a plurality of key distribution centers and the E-mail transmission program can choose either one of the centers to ask for the certificate of the second user, and wherein the centers are connected in a network which is hierarchical with respect to endorsement of the public key of each center, so that the public key of any center is endorsed in a certificate signed by the private key of a center higher in the hierarchy, up to one center at the highest level.

3. The secure electronic mail method according to claim 1, wherein there are a plurality of key distribution centers and the E-mail transmission program can choose either one of the centers to ask for the certificate of the second user, and wherein the centers are connected in a network capable of automatic exchange of certificates between the centers so as to locate a certificate for any desired second user which may be stored in any one of the centers, and for transferring the certificate to another center to be delivered to the first user.

4. A secure method for sending a first message from a first user to a second user as a business registered electronic mail (BRM), comprising the following steps:

a. the first user prepares the first message to be sent, indicates the identification of the second user to whom the first message is to be sent, and activates an E-mail transmission program in their computer;

b. the BRM E-mail transmission program at the first user automatically connects to the Internet, connects there to one of the key distribution centers and asks for the public key of the second user;

c. the center sends a certificate to the first user, wherein the certificate includes the public key for the second user together with identifying information for the second user, all encrypted with the private key of the center;

d. the E-mail program at the first user decrypts the certificate to retrieve a public key for the second user;

e. the E-mail program at the first user creates a second message which includes a message section including the first message to be sent which is encrypted with the public key for the second user, a hash or CRC of the message section, and a sender identification section with information to identify the first user;

f. the E-mail program at the first user sends the second message to the E-mail address of the second user;

g. when the second user connects to Internet to retrieve messages in their E-mail, a BRM E-mail transmission program at the second user automatically presents information relating to the received second message;

h. the second user is given a choice, either to accept or not the message. If the second user decides not to accept the second message, then END; otherwise the E-mail program at the second user automatically decrypts the second message with the private key of the second user, presents the decrypted message to the second user, prepares a third

message including a receipt for the second message signed with the private key of the second user, wherein the receipt includes the identification of the message and the hash or CRC and additional optional information, and the second user sends the third message to the E-mail address of the first user.

5. The secure method according to claim 4, wherein the sender identification section in the second message includes a certificate with the public key of the first user, signed by a key distribution center.

6. The secure method according to claim 4, wherein the sender identification section in the second message includes a name or pseudonym which identifies the first user, and the second message further includes a general information section comprising a CRC or hash and/or other information, all encrypted with the private key of the first user; and wherein the E-mail program in the second user automatically connects to a key distribution center to retrieve the public key of the first user, which key is used to decrypt the general information section; if the CRC or hash and/or the other information therein corresponds to that computed by the E-mail of the second user, then will the second user send the third message to the first user.

7. The secure method according to claim 4, wherein there are a plurality of key distribution centers and the E-mail transmission program can choose either one of the centers to ask for the certificate of the second user, and wherein the centers are connected in a network which is hierarchical with respect to endorsement of the public key of each center, so that the public key of any center is endorsed in a certificate signed by the private key of a center higher in the hierarchy, up to one center at the highest level.

8. A secure method for sending a first message from a first user to a second user as a legal registered electronic mail (LRM), comprising the following steps:

a. the first user prepares the first message to be sent, indicates the identification of the second user to whom the first message is to be sent and an intermediary or post office (PO) for the transmission, and activates an E-mail transmission program in their computer;

b. the LRM E-mail transmission program at the first user automatically prepares a second message including the first message which is encrypted for example with a symmetrical key and algorithm, together with a general information section including a serial number or message identification and information relating to the public key of the second user, together with a CRC or hash and optional time/date information.

c. the LRM E-mail transmission program at the first user automatically prepares a third message including the decryption key for the first message, encrypted with the public key of the second user, together with a general information section including a serial number or message identification, together with the CRC or hash and optional time/date information;

d. the LRM E-mail transmission program at the first user automatically prepares a fourth message including a notice that an E-mail message was sent to the second user, the CRC or hash of the message, the identification of the intermediary and the serial number or message identification;

e. the LRM E-mail transmission program at the first user sends the third message to the chosen intermediary or PO, the fourth message to the second user and the second message either to the intermediary or the second user;

f. when the second user connects to Internet to retrieve messages in their E-mail, a LRM E-mail transmission program at the second user automatically presents information relating to the received message;

g. the second user is given a choice, either to accept or not the message. If the second user decides not to accept the second message, then END; otherwise the E-mail program at the second user automatically encrypts the fourth message with the private key of the second user to create a fifth message, and sends the fifth message to the intermediary or PO, so that the fifth message is a receipt signed by the second user,

with the receipt including the message identification and the CRC or hash relating to the contents of the message.

h. the intermediary decrypts the fifth message with a public key of the second user, and compares with the message identification in the third message; if the two correspond, then the intermediary sends the third message with the decryption key therein to the second user, and the fifth message with the receipt from the second user is made available to the first user; if the second message with the encrypted message itself was sent to the intermediary, then the intermediary sends the second message to the second user.

9. The secure method according to claim 8, wherein there are a plurality of intermediaries or POs, and the E-mail transmission program can choose either one of the intermediaries to act as PO for a given transmission, and wherein the intermediaries are connected in a network which is hierarchical with respect to endorsement of the public key of each center and intermediary, so that the public key of any intermediary is endorsed by a certificate issued by a key distribution center, and each center is endorsed in a certificate signed by the private key of a center higher in the hierarchy, up to one center at the highest level.

10. The secure method according to claim 8, wherein the LRM E-mail transmission program at the first user automatically extracts the public key for the intermediary and/or the second user by connecting to a key distribution center on internet and asking for a certificate for the

intermediary and/or second user, and wherein the public key in the certificate or certificates is used in the subsequent transaction with the entity to which that key belongs.

11. The secure method according to claim 8, wherein the LRM E-mail transmission program at the second user automatically challenges the intermediary for its key by receiving a message encrypted with the private key of the intermediary and decrypting with the public key thereof, and wherein the fifth message in step (g) is sent to the intermediary or PO only if the keys of the intermediary correspond.

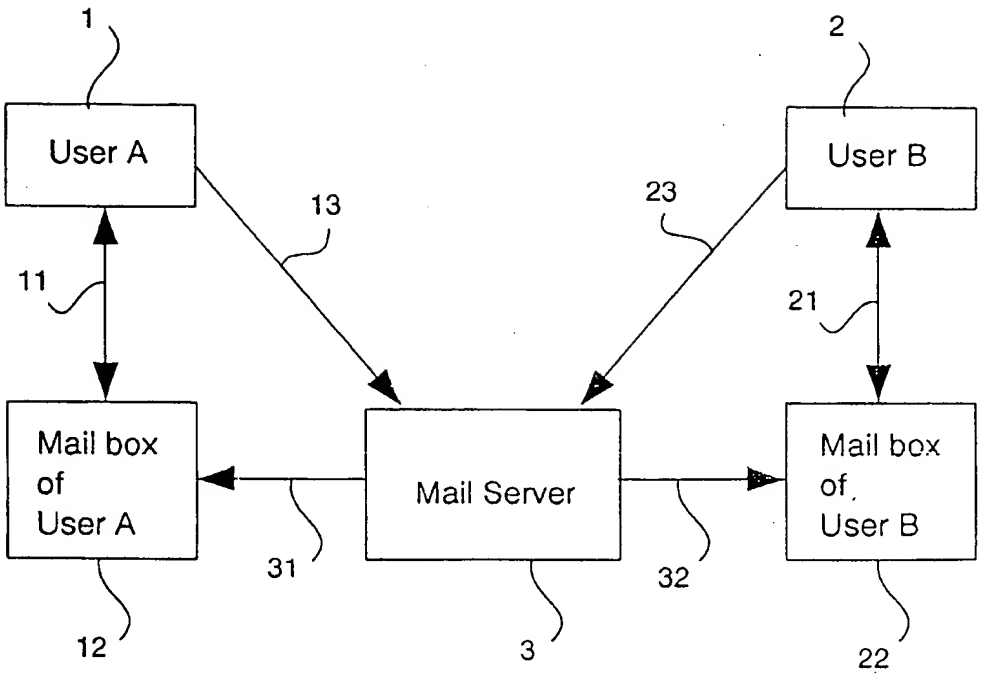

1
2
User A
User B
13
23
11
21
Mail box of User A
Mail Server
Mail box of User B
31
32
12
3
22

Fig. 1

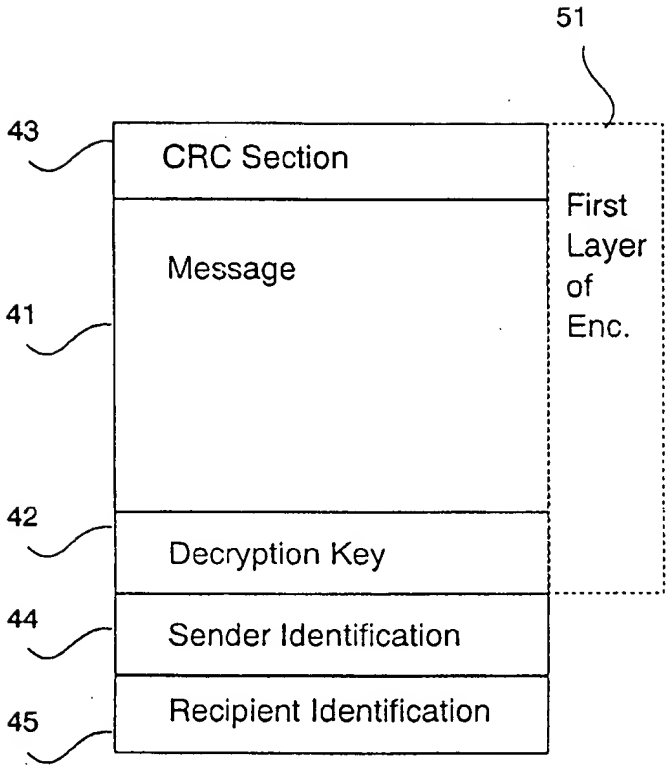

51
43
CRC Section
Message
41
First Layer of Enc.
42
Decryption Key
44
Sender Identification
45
Recipient Identification

Fig. 2

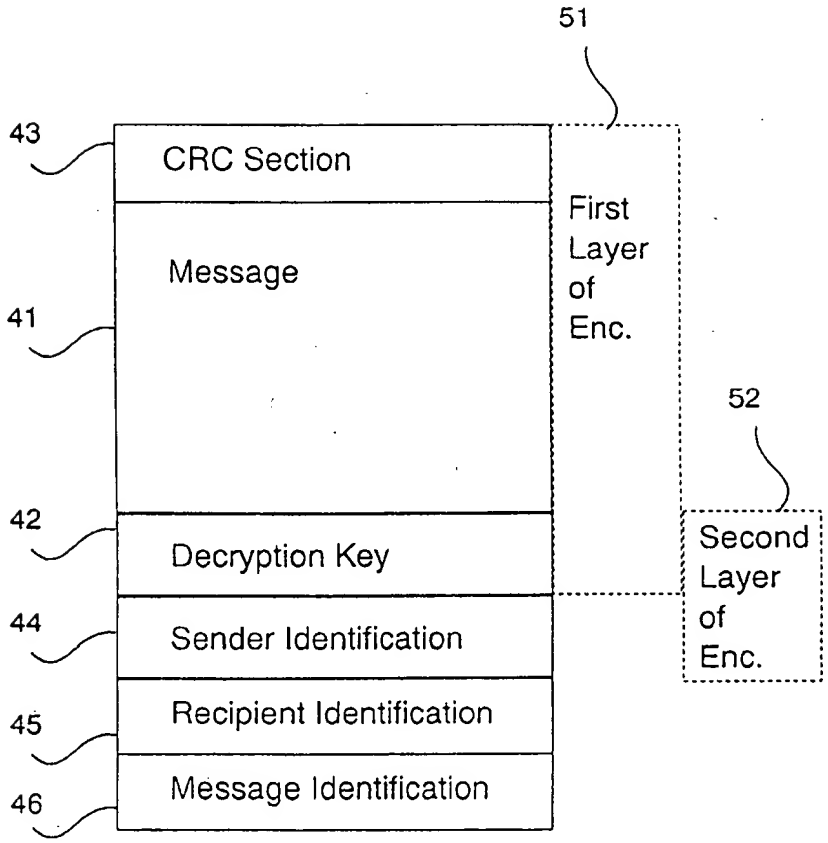

51
43
CRC Section
Message
41
First Layer of Enc.
52
42
Decryption Key
Second Layer of Enc.
44
Sender Identification
45
Recipient Identification
46
Message Identification

Fig. 3

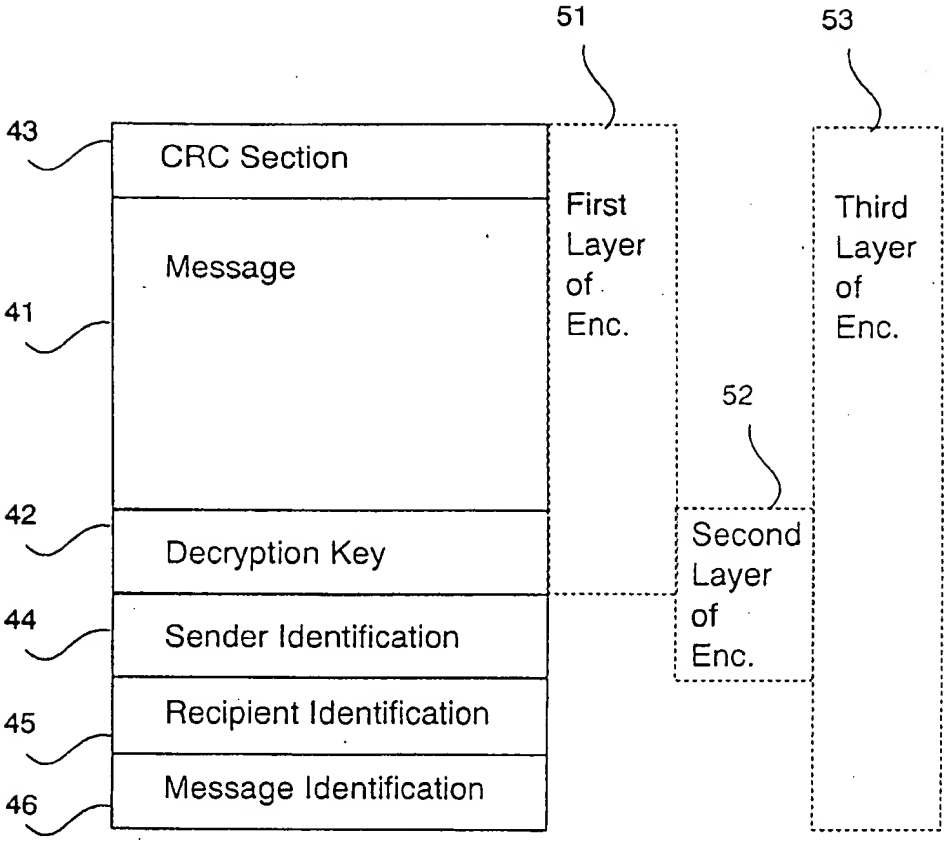

51
53
43
CRC Section
Message
41
First Layer of Enc.
52
Third Layer of Enc.
42
Decryption Key
Second Layer of Enc.
44
Sender Identification
45
Recipient Identification
46
Message Identification

Fig. 4

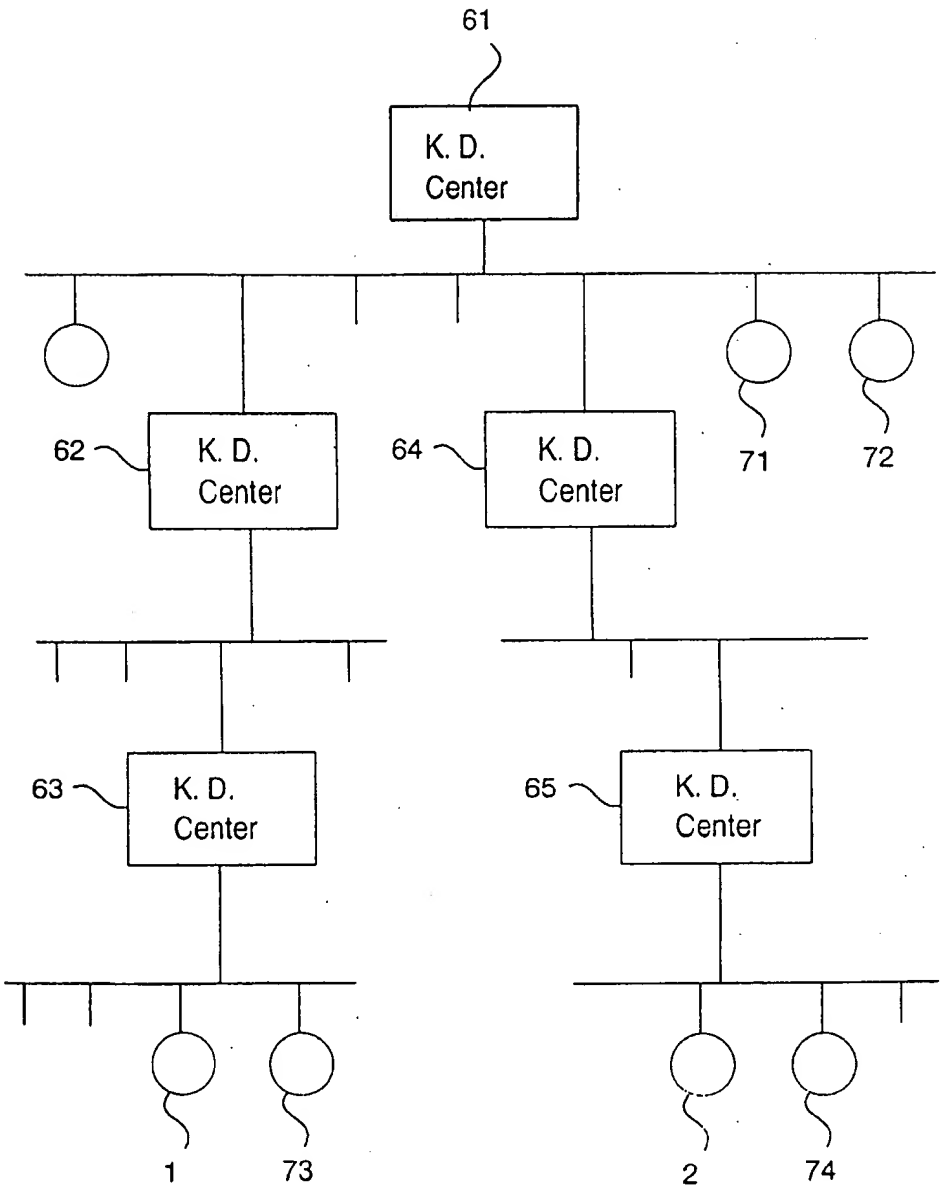

61
K. D. Center
62
K. D. Center
64
K. D. Center
71
72
63
K. D. Center
65
K. D. Center
1
73
2
74

Fig. 5